Leftover Items from TAC's consideration of EA Table Updates

AREA: Stored Data Encryption

Exec branch standards are divided by type 1) Full-Disk encryption, 2) File (Folder) encryption, 3) Mass storage encryption, and 4) Database encryption and 5) Encryption on removable devices and drives. No technical standards are specified only some, functional standards for each and 25 general requirements for all.

1) includes the entire operating system, all applications, and all data/information. Full-disk encryption software contains components that are independent of the operating system and execute before the operating system is loaded as well as authentication.
2) Provide automatic security in which each new file/folder encryption capability must be manually turned off/on.
3) Applies throughout the lifecycle of all data/information, methods used must have both logical and physical segmentations; provide efficient encryption/decryption across multiple mass storage device types including fiber channel disks within an IP based network environment.
4) Can apply to entire database, or by calling functions, or stored procedures and database triggers, or natively using Database Management Systems (DBMS) encryption features to encrypt all or in part (column, row, or field level).
5) USB flash-drives must have password/security capabilities built into the device. USB flash-drives and removable storage devices may be bought with encryption software installed or software can be purchased / installed after-the-fact.

Rather than identifying a standard product to meet all the requirements, the executive branch has identified two vendors on state contract to provide various encryption solutions: South Seas Corp and Accuvant Inc.

AREA: e-mail encryption

Exec branch standard is Secure /Multipurpose Internet Email Extension (S/MIME) or PGP

TAC members recommended www.globalcerts.net, a secure e-mail gateway solution, either as an appliance or hosted. They also asked what met HIPAA requirements. HIPAA is vague – it applies the same functional standards to the electronic presentation of patient information as it applies to paper presentation and leaves the technical solution up to the provider, subject to audit.

AREA: e-Signature on AOC forms

Exec branch standard is PKI or PGP for full, electronic signing of documents (Office of Secretary of State has statutory and policy authority for electronic signatures per A.R.S. § 41-132)

MS-Office Digital Signature (2007+) and Adobe Digital IDs (for PDF forms) are used by AOC today. These are both self-certifications, and do not ensure document integrity , just password protection of the credential on the machine it was created on. Note that I can call myself anyone I want when establishing the signature – the software performs no identity check like a third party would. No keys are involved like with PKI, but no expense is involved, either.

AREA: File Transfer protocol

Issue: FTP is inherently unsafe (no method is specified for transferring data in an encrypted fashion) and unreliable so was prohibited in previous iterations of the table. MQ is the courts' file transfer solution. Very few local courts consider MQ a viable alternative and have therefore continued using FTP.

Exec Branch allows it in OSI Layers 6 and 7.

Ideas: The common solution to the lack of security is to use either SFTP (SSH File Transfer Protocol), or FTPS (FTP over SSL), which adds SSL or TLS encryption to FTP as specified in RFC 4217.

It is possible, similar to the case of MS-Access, to separate ad hoc, non-production use from scheduled, recurring production transfers of data. The requirement for MQ would stand in the area of production transfers but ftp could still be allowed in the ad hoc, non-production space.